UNIVERSIDADE FEDERAL DA PARAÍBA
DEPARTAMENTO DE CIÊNCIAS EXATAS
INTRODUÇÃO À TEORIA DOS NÚMEROS - 2010.1
PROFESSOR: GIVALDO DE LIMA

MÁXIMO DIVISOR COMUM - AULA 12

Definição: Sejam a e b dois números inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$). Chama-se máximo divisor comum de a e b, o número inteiro positivo d que satisfaz:

- (i) $d|a$ e $d|b$;
- (ii) Se $c|a$ e se $c|b$, então $c \leq d$.

Pela definição acima podemos observar que por (i) d é um divisor comum entre a e b, e por (ii), d é o maior dentre todos os divisores comuns de a e b.
Notação:

$$mdc(a, b).$$

Observações:

- $mdc(a, b) = mdc(b, a)$
- $mdc(0, 0) \nexists$
- $mdc(a, 1) = 1$
- Se $a \neq 0$, então $mdc(a, 0) = |a|$
- Se $a|b$, então $mdc(a, b) = |a|$.

Exemplos:

- a) $mdc(8, 1) = 1$
- b) $mdc(-3, 0) = |-3| = 3$
- c) $mdc(-6, 12) = |-6| = 6$
- d) $mdc(16, 24) =?$
  $D(16) = \{\pm1, \pm2, \pm4, \pm8, \pm16\}$
  $D(24) = \{\pm1, \pm2, \pm3, \pm4, \pm6, \pm8, \pm12, \pm24\}$
  $D(16, 24) = \{\pm1, \pm2, \pm4, \pm8\}$
  Portanto,
  $$mdc(16, 24) = 8$$

Obs.:

$$mdc(a, b, c) = mdc(mdc(a, b), c)$$

Teorema: (Existência e Unicidade do MDC)

Se a e b são dois números inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$), então existe e é único o $mdc(a, b)$; além disso, existem números inteiros x, y tais que $mdc(a, b) = a.x + b.y$, ou seja, o $mdc(a, b)$ é uma combinação linear de a e b.

Demonstração:

Seja $S = \{a.u + b.v : a.u + b.v > 0,\ u,\ v\ \in \mathbb{Z}\}$.
Note que $S \neq \varnothing$, pois se, por exemplo, $a \neq 0$, então um dos dois inteiros

$$a = a.1 + 0 \ \text{ e } \ -a = a.(-1) + 0$$

é positivo, e portanto pertence a S.

Pelo Princípio da Boa Ordenação, existe e é único o elemento d de S, tal que $d = a.x + b.y,\ \ x,\ y\ \in \mathbb{Z}$.
Vamos mostrar que $d = mdc(a, b)$.
Pelo Algoritmo da Divisão, temos que

$$a = d.q + r,\ 0 \leq r < d$$

$$\Rightarrow r = a - d.q = a - (a.x + b.y).q = a.(1 - x) + b.(-q.y),$$

ou seja, r é combinação linear de a e b. Como $0 \leq r < d$ e $d > 0$ é o elemento mínimo de S, segue que $r = 0$ e consequentemente $a = d.q \Rightarrow d|a$.
De modo análogo $d|b$.

Portanto, d é um divisor comum positivo de a e b. Finalmente, se c é um divisor comum de a e b ($c|a$ e $c|b,\ c > 0$), então

$$c|(a.x + b.y) \Rightarrow c|d \Rightarrow c \leq d.$$

Ou seja, d é o maior divisor comum positivo de a e b.
Portanto, $d = mdc(a, b) = a.x + b.y,\ \ x,\ y\ \in \mathbb{Z}$.

Exemplos:

a) $mdc(6, 27) = 3 = 6.(-4) + 27.1$

b) $mdc(-8, -36) = 4 = (-8).4 + (-36).(-1)$

Definição:

Sejam a e b dois números inteiros não conjuntamente nulos. Diz-se que a e b são números primos entre si, se e somente se o $mdc(a, b) = 1$.

Exemplos:

a) 2 e 5 são primos entre si;

b) -9 e 16 são primos entre si;

c) 27 e 45 não são primos entre si.

Vejam algumas aplicações!!!!

1. Prove que a e b, sendo inteiros não conjuntamente nulos, são primos entre si, se e somente se existem inteiros x e y tais que $a.x + b.y = 1$.
Solução:

- ($\Rightarrow$) Sendo a e b primos entre si, então o $mdc(a.b) = 1$, o que significa que existem $x,\ y\ \in \mathbb{Z}$ tal que $a.x + b.y = 1$.
- ($\Leftarrow$) Se existem inteiros x e y tais que $a.x + b.y = 1$ e se o $mdc(a, b) = d$, então $d|a$ e $d|b$. Dessa forma, $d|(a.x + b.y) \Rightarrow d|1 \Rightarrow d = 1$, ou seja, $mdc(a, b) = 1$ o que nos mostra que a e b são primos entre si.

$\blacksquare$

2. Prove que se $mdc(a, b) = d$, então $mdc(\frac{a}{d}, \frac{b}{d}) = 1$.
Solução:

- Observe que $\frac{a}{d}$ e $\frac{b}{d}$ são números inteiros.
- Como $mdc(a, b) = d$, existem inteiros x e y tais que $a.x + b.y = d$.
- Dividindo essa equação por d, temos que

$$(\frac{a}{d}).x + (\frac{b}{d}).y = 1$$

e, pelo exemplo 1, segue que $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si.
Portanto,

$$mdc(\frac{a}{d}, \frac{b}{d}) = 1.$$

$\blacksquare$

3. Prove que se $a|b$ e se $mdc(b, c) = 1$, então $mdc(a, c) = 1$.
Solução:

- Como $a|b \Rightarrow b = a.q, \quad q \in \mathbb{Z}$
- Como $mdc(b, c) = 1 \Rightarrow b.x + c.y = 1,\ x,\ y \in \mathbb{Z}$
- Portanto,

$$a.q.x + c.y = 1 \Rightarrow a.(q.x) + c.y = 1 \Rightarrow mdc(a, c) = 1$$

$\blacksquare$

4. Prove que se $a|c$, se $b|c$ e se $mdc(a, b) = 1$, então $ab|c$.
Solução:

- Como $a|c \Rightarrow c = a.q_1,\ q_1 \in \mathbb{Z}$
- Como $b|c \Rightarrow c = b.q_2,\ q_2 \in \mathbb{Z}$
- Como $mdc(a, b) = 1 \Rightarrow a.x + b.y = 1,\ x,\ y \in \mathbb{Z}$
- Multiplicando essa equação por c, temos

$$ac.x + bc.y = c \Rightarrow a.(bq_2).x + b.(aq_1).y = c \Rightarrow$$

$$\Rightarrow ab.(q_2.x + q_1.y) = c$$

Portanto,

$$ab|c.$$

$\blacksquare$

5. Prove que se $mdc(a,b) = 1 = mdc(a,c)$, então $mdc(a,bc) = 1$.
Solução:

- Como $mdc(a,b) = 1 \Rightarrow a.x + b.y = 1,\ x,\ y\ \in \mathbb{Z}$.
- Como $mdc(a,c) = 1 \Rightarrow a.z + c.t = 1,\ z,\ t\ \in \mathbb{Z}$.
- Daí, note que

$$1 = ax + by.1 = ax + by.(az + ct) = a(x + byz) + bc(yt)$$

$$\Rightarrow mdc(a,bc) = 1.$$

■

6. Prove que se $mdc(a,bc) = 1$, então $mdc(a,b) = 1 = mdc(a,c)$.
Solução:

- Como $mdc(a,bc) = 1 \Rightarrow a.x + bc.y = 1,\ x,\ y\ \in \mathbb{Z}$.
- Mas, se $ax + bc.y = 1 \Rightarrow ax + b(cy) = 1 \Rightarrow mdc(a,b) = 1$.
- Mas, $ax + bcy = 1 \Rightarrow ax + c.(by) = 1 \Rightarrow mdc(a,c) = 1$

■

7. Prove que se $a|bc$ e se $mdc(a,b) = 1$, então $a|c$
Solução:

- Como $a|bc \Rightarrow bc = a.q,\ q \in \mathbb{Z}$
- Como $mdc(a,b) = 1 \Rightarrow ax + by = 1,\ x,\ y\ \in \mathbb{Z}$
- Daí,

$$ac.x + bc.y = c \Rightarrow acx + aq.y = c \Rightarrow a.(cx + qy) = c \Rightarrow a|c.$$

■